REMARKS/ARGUMENTS

Claims 1-36 stand rejected in the outstanding Official Action. Claims 3, 6, 10, 15, 18, 22, 27, 30 and 34 have been cancelled without prejudice and claims 1, 4, 5, 7-9, 11-13, 19-21, 23-25, 28, 29, 31-33, 35 and 36 have been amended. Therefore, claims 1, 2, 4, 5, 7-9, 11-14, 16, 17, 19-21, 23-26, 28, 29, 31-33, 35 and 36 are the only claims remaining in this application.

The Examiner has suggested that the original title of the patent application was not descriptive of the invention. Applicants have amended the title to read "Heuristic Detection of Polymorphic Computer Viruses Based on Redundancy in Viral Code" which is based upon the operation of the invention. Entry of this title change is respectfully requested. Should the Examiner believe another title to be more descriptive of the claimed invention, Applicants will certainly consider any such suggestion.

Claims 12, 24 and 36 are objected to as including a minor informality as correctly noted by the Examiner. The word "exceed" has been amended to read "exceeded" in each of these claims. Therefore, any further objection to these claims has been obviated.

Applicants have amended independent claim 1 to include the limitations of previous claims 3, 6 and 10 and has made similar amendments to the other independent claims. As a result, each of the independent claims not only includes the original features, but also the features that the analysis logic includes a dependence table (from claim 3), the analysis logic marks certain variables in reliance upon information in the dependence table (claim 6) and the analysis logic parses the executable computer program for suspect program instructions and taking the appropriate action (claim 10). In effect, amended claim 1 is an independent version of claims 3, 6 and 10 combined. Similar amendments have been made to the other independent

claims 13 and 25 (claim 13 incorporating the subject matter of claims 15, 18 and 22 and claim 25 incorporating the subject matter of claims 27, 30 and 34).

It will be seen by comparison of the limitations in claims 1, 13 and 25, as currently amended, are not disclosed or rendered obvious in the cited Yann and Nachenberg references. It is noted that in the outstanding Official Action, the Examiner admits that Yann **does not disclose** "the use of an orderly dependence table to store the state variables, or registers, and their dependency on particular variables" (page 5, lines 26-27) with respect to the subject matter of claims 3, 15 and 27. This admission is appreciated.

The Examiner also admits that the marking limitation as dependent on a new value "**is lacking** in Yann because Yann lacks an actual table for monitoring the registers or state variables in the loaded values" (emphasis added, page 6, lines 18-20) which are characteristics of former claims 6, 18 and 30, now incorporated into independent claims 3, 13 and 25. This admission is also appreciated.

Additionally, the Examiner admits that "Yann **fails to disclose** the method of following each branch of a branching point to determine suspicious behavior" (emphasis added, page 7, lines 15-16) referring to the subject matter of claims 10, 22 and 34, now incorporated into claims 1, 13 and 25. This admission is also very much appreciated.

Applicants' claimed "dependency table" tracks the dependency between state variables within the computer and loaded variable values. While the Examiner has taken a simplistic view of that taught in former claims 10, 22 and 34, now incorporated into amended claims 1, 13 and 25, it is submitted that these claims require more than merely "following all branches" as suggested by the Examiner. The claim language states that "upon occurrence of a branch first

following a first branch path having saved pending analysis results and subsequently returning to follow a second branch path **having restored said pending analysis results**." (emphasis added). Thus, the subject matter of amended claims 1, 13 and 25 now requires restoring "said pending analysis results."

The Examiner does not allege that Yann or Nachenberg disclose anything remotely related to restoring "said pending analysis results." This is clearly recited as a requirement and an important portion of Applicants' invention.

Additionally, applicants' recited dependency table in amended claims 1, 13 and 25 is a convenient way to track all of the data values globally. There is no disclosure in any cited prior art reference of the manner in which multiple copies of the tables are used during multiple branch processing. The well-known manner of branch processing described in Nachenberg is insufficient to accommodate the operation with multiple tables during multiple branch processing. Nachenberg simply does not reflect the actual dependencies between adjacent execution branches and execution loops.

If the Yann and Nachenberg disclosures were combined and Nachenberg's teachings followed, the dependency information in the stored dependency tables for the branches would be unreliable. Nachenberg's technique is mostly aimed at finding bad code hidden somewhere among a program's code branches (hence the simplicity of tracing the code flows in Nachenberg), but not to apply this in Yann's analysis looking for code redundancies, i.e., unknown bad code. Some code redundancies may only appear across multiple branches, i.e., one path through code flow is not sufficient to determine if the code is useful or useless for sure without looking through alternative paths.

Considering the rejection of claims 10, 22 and 34 (which claim limitations have been incorporated into claims 1, 13 and 25), the only basis for rejection of these claims is under 35 USC §103 over the Yann/Nachenberg combination. The Examiner suggests that it would be obvious to one of ordinary skill in the art to combine Nachenberg with Yann and then "add a method to explore infectious codes in an untaken branching point as a further security measure to examine whether code is viral." How or where the Examiner believes there is any "reason" or "motivation" to combine the Yann and Nachenberg references is not set forth in the Official Action and therefore the rejection under §103 fails.

Moreover, the Examiner has not indicated the source for why he believes it would be obvious to "add a method to explore infectious code" which he is combining with the Yann/Nachenberg combination in his rejection on page 7, lines 20-22. Absent a detailed disclosure of how and where either Yann or Nachenberg teaches Applicants' "dependence table," the interrelationship of the dependence table with the other structures and processes of the independent claims, or where the "method to explore infectious code" came from, there is simply no *prima facie* case of obviousness under 35 USC §103 and any further rejection of independent claims 1, 13 and 25 is respectfully traversed. Inasmuch as all remaining claims depend directly or indirectly upon independent claims 1, 13 and 25, they are also believed allowable.

In support of his rejection of claims 11, 23 and 35, the Examiner contends that "it is inherent in Nachenberg that the entire branch path is followed to detect infectious code." (Page 8, line 3). This inherency contention is respectfully traversed and pursuant to the Manual of Patent Examining Procedure (MPEP) Section 2144.03, where the applicant traverses an assertion of inherency or "official notice of facts outside of the record," the MPEP requires the

Examiner to "cite a reference in support of his or her position." Accordingly, Applicants' traversal requires the Examiner to cite a reference in support of the alleged inherency recited on page 8, line 3. Applicant also applies this MPEP provision to the Examiner's assertion that use of the "method to explore infectious code" would somehow be obvious to add to the Yann/Nachenberg combination as noted above.

Having responded to all objections and rejections set forth in the outstanding Official Action, it is submitted that the remaining claims are in condition for allowance and notice to that effect is respectfully solicited. In the event the Examiner is of the opinion that a brief telephone or personal interview will facilitate allowance of one or more of the above claims, he is respectfully requested to contact Applicants' undersigned representative.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100